CLOUDFLARE

BIAŁA KSIĘGA

Przewodnik dotyczący złośliwych botów: wczesne sygnały ostrzegawcze i niezbędne działania

Spis treści

Wprowadzenie

Boty stanowią obecnie około 30% ruchu w Internecie. Wiele z nich ma na celu szkodzenie organizacjom takim jak Twoja. Szacuje się, że 93% ruchu generowanego przez boty jest niezidentyfikowane i potencjalnie złośliwe. Pozyskiwanie treści i cen, przejęcia kont, ataki typu „credential stuffing", „credit card stuffing" i „inventory hoarding", a także oparte na sieciach botów ataki DDoS — wszystko to wskazuje, że złośliwe boty z roku na rok stają się coraz bardziej złożone i wyrafinowane.

Co więcej, tradycyjne metody walki z botami, takie jak blokowanie lokalizacji, blokowanie adresów IP i tradycyjne CAPTCHA, są obecnie nieskuteczne. Mechanizmy CAPTCHA są wręcz łatwiejsze do rozwiązania dla botów niż dla ludzi.[1]

Z tego powodu żadna pojedyncza taktyka nie może powstrzymać każdego bota i zapobiec szkodom wyrządzanym Twoim użytkownikom oraz Twojej marce. Jedynym skutecznym sposobem jest wyczulenie na różnorodne charakterystyczne oznaki ostrzegawcze wskazujące na aktywność botów oraz reagowanie na każdą z nich poprzez gromadzenie danych, a następnie wdrażanie ukierunkowanych działań, wykrywanie wzorców, analizę predykcyjną i inne uzupełniające strategie.

1. https://www.usenix.org/conference/usenixsecurity23/presentation/searles

Sygnały ostrzegawcze wskazujące na problem z botami

Śledząc szereg potencjalnych wskaźników, masz duże szanse na wykrycie złośliwych botów, zanim zdążą wyrządzić poważne szkody. Oto, na co należy zwrócić uwagę:

Wyższe koszty infrastruktury bez wzrostu zakresu działalności

Cały ruch do Twojej witryny wiąże się z pewnymi kosztami. Niezależnie od tego, kto lub co uzyskuje dostęp do Twoich treści, koszty przechowywania i przetwarzania obciążają Ciebie. Złe boty mogą zwiększać koszty związane z ruchem sieciowym, nie przynosząc firmie żadnych zysków. Podczas gdy dobre boty są używane przez wyszukiwarki do indeksowania zawartości Twojej witryny, wspierając tym samym jej pozycję w wynikach SEO, złe boty generują każdego roku znaczne, nadmierne koszty związane z przepustowością.

Nietypowe zakupy małych ilości pożądanych pozycji

Jeśli zauważysz, że podejrzanie wysoki odsetek Twojego asortymentu jest sprzedawany zaskakująco wąskiej grupie kupujących, przyczyną mogą być boty prowadzące atak typu inventory hoarding. Podczas gdy niektóre z tych botów po prostu wypełniają i porzucają koszyki, blokując w ten sposób dostęp dla prawdziwych klientów, inne faktycznie kupują Twoje produkty, aby następnie odsprzedać je drożej na innych stronach.

Więcej skarg klientów

Wzrost liczby zgłoszeń do działu pomocy technicznej w związku z blokadami kont i oszukańczymi transakcjami może wskazywać na ataki typu „credential stuffing” z użyciem botów. Podczas takiego ataku boty przejmują legalne konta użytkowników, wykorzystując informacje uzyskane z wcześniejszych wycieków danych. Oprócz negatywnego wpływu na doświadczenie klienta, te nieuczciwe transakcje przeciążają Twoje serwery, powodując wydłużenie czasu ładowania stron, a nawet niedostępność witryny.

Wzrost liczby nieudanych prób logowania

Każdemu klientowi zdarza się od czasu do czasu pomylić hasło – jeśli jednak zauważysz nagły wzrost liczby nieudanych prób logowania, najprawdopodobniej masz problem z botami. Podczas gdy niektóre boty wykorzystujące atak typu „credential stuffing” próbują uzyskać dostęp do legalnych kont klientów za pomocą skradzionych danych uwierzytelniających, prostszą i bardziej powszechną techniką jest przeprowadzenie ataku metodą brute force, w którym boty próbują masowo logować się, używając słowników zawierających tysiące popularnych nazw użytkowników i haseł. Gdy bot przekroczy limit nieudanych prób logowania do konkretnego konta w Twojej witrynie, prawdziwy właściciel tego konta zostanie zablokowany do czasu rozwiązania problemu — co stanowi poważny problem dla takiego użytkownika.

Niski zwrot z wydatków na reklamę

Reklama cyfrowa może być skutecznym narzędziem do generowania ruchu w Twojej witrynie, ale jest również przydatną bronią dla złośliwych botów. Wiele botów generujących sztuczny ruch imituje zachowania prawdziwych użytkowników – wielokrotnie klika w reklamy, aby zwiększyć koszty kampanii z płatnościami za kliknięcie (PPC), a następnie opuszcza stronę bez dokonania zakupu. Chociaż niektóre platformy reklamowe wdrożyły algorytmy uczenia maszynowego w celu ograniczenia oszustw typu click fraud, duża ich część pozostaje niewykryta.[2] Dlatego tak ważne jest, aby aktywnie działać i monitorować każde kliknięcie pochodzące z Twoich reklam.

Nierzetelne statystyki wyświetleń strony

Jeśli liczba odsłon Twojej witryny gwałtownie rośnie bez wyraźnego powodu, przyczyną mogą być złośliwe boty. Chociaż wzrost ruchu może pochodzić od użytkowników, jeśli właśnie wprowadzono na rynek nowy produkt lub rozpoczęto promocję wydarzenia, operatorzy złośliwych botów coraz sprytniej używają ich do pozyskiwania danych dokładnie w takich momentach, kradnąc zawartość i negatywnie wpływając na zagregowane dane analityczne.

Nagły wzrost liczby zakładanych kont

Kiedy nagle pojawiają się setki lub nawet tysiące nowych kont użytkowników, przyczyną tego napływu mogą być boty. Te fałszywe profile mogą być wykorzystywane do spamowania Twoich publicznych ocen i popełniania wielu innych oszustw, co zagraża nie tylko Twoim przychodom i utrzymaniu użytkowników, ale także wiarygodności Twojej marki.

Duplikaty Twoich treści w niezatwierdzonych witrynach

Udostępnianie Twoich treści w innych witrynach może być zjawiskiem pozytywnym, ale nagły wzrost liczby jawnych duplikatów treści jest znakiem rozpoznawczym działania botów pozyskujących dane. Kradną one informacje, które gromadzisz i starannie wybierasz, umożliwiając operatorom złośliwych witryn ich hostowanie we własnych domenach, co zwiększa ich ruch kosztem Twojego.

Ruch pochodzący z nietypowych lokalizacji geograficznych

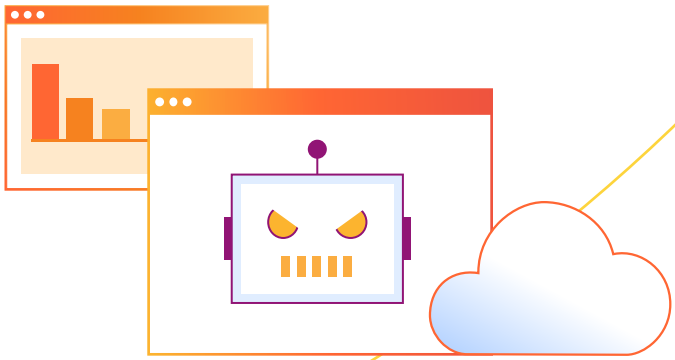
Nagłe skoki aktywności pochodzące z nieoczekiwanych lokalizacji mogą wskazywać na aktywność złych botów — zwłaszcza, jeśli ta aktywność występuje w skupiskach, zlokalizowanych w regionach, w których nie mieszkają Twoi klienci lub Twoje usługi nie są dostępne. Obserwuj uważnie wszelką podejrzaną aktywność, która wydaje się niepowiązana z Twoją zwykłą bazą użytkowników.

Ruch z typowych lokalizacji w nietypowych godzinach

Podobnie jak nagłe wzrosty ruchu z nieoczekiwanych lokalizacji mogą wskazywać na złośliwe boty, gwałtowne wzrosty ruchu z normalnych lokalizacji w nietypowych porach mogą być objawem działania botów próbujących podszywać się pod Twoich zwykłych użytkowników. Jeśli na przykład zauważysz nagły wzrost aktywności z typowego regionu w środku nocy, zbadaj dokładniej ten ruch.

Wzrost liczby błędów weryfikacji kart

Szczególnie niebezpiecznym sygnałem wskazującym na obecność złośliwych botów jest wzrost liczby transakcji kartą kredytową, które nie przechodzą weryfikacji. Boty wykorzystujące metodę „credit card stuffing" testują tysiące skradzionych numerów kart kredytowych, aby znaleźć działający numer. Osiągają to poprzez dokonywanie drobnych zakupów w mniej zabezpieczonych witrynach internetowych, a następnie przeprowadzanie większych transakcji w bardziej renomowanych serwisach lub sprzedaż zweryfikowanych numerów kart w dark webie. Twoja witryna może być elementem tych działań na każdym etapie łańcucha, a jeśli liczba nieudanych transakcji będzie wystarczająco duża, dostawca usług płatniczych może nałożyć na Ciebie karę.



2. https://www.entrepreneur.com/article/313943

Taktyki zwalczania botów

Ponieważ nie ma dwóch identycznych ataków botów, zazwyczaj potrzebna jest kombinacja różnych taktyk, aby skutecznie je powstrzymać. Rozważ następujące strategie:

Blokuj szkodliwe boty, gdy tylko je wykryjesz

Najbardziej oczywistą i skuteczną reakcją na boty jest zablokowanie całego ruchu, który został zidentyfikowany jako pochodzący z aktywności złośliwych botów. Już sama ta taktyka może przynieść znaczne oszczędności kosztów w zakresie przepustowości i przechowywania danych, a także zapewnić ochronę zaufania klientów oraz reputacji Twojej marki. Pamiętaj jednak, że jeśli operator bota jest wysoce zmotywowany, może zmienić taktykę i powrócić później z inną strategią ataku.

Umieść wszystkie znane Ci dobre boty na liście dozwolonych

Nawet jeśli wykrywasz i blokujesz złe boty, ważne jest, aby dbać o to, aby dobre boty z wyszukiwarek od partnerów nadal były w stanie indeksować Twoją witrynę. Zapewnia to utrzymanie odpowiedniego rankingu SEO oraz płynny przepływ prawidłowego ruchu klientów od zewnętrznych usługodawców, którzy kierują ruch do Ciebie. Dodanie botów do listy dozwolonych znacznie ułatwia również ustawianie reguł blokowania botów, tak aby nie wpływało to negatywnie na dostęp prawdziwych użytkowników.

Weryfikuj wykryte podejrzane boty

Gdy tylko zauważysz wzorzec podejrzanych logowań, niską głębokość przechodzenia przez witrynę lub krótki czas spędzony na stronie, nieudane próby weryfikacji kart kredytowych bądź też inne zachowania charakterystyczne dla botów, wdróż test bezpieczeństwa. W przeszłości wysyłanie testów CAPTCHA było uważane za dobrą praktykę. Jednak wiele zaawansowanych botów potrafi teraz rozwiązywać te łamigłówki szybciej i dokładniej niż ludzie.

Obecnie najlepszym rozwiązaniem jest stosowanie wyzwań niewymagających CAPTCHA, w których oprogramowanie weryfikujące uwzględnia wiele czynników, aby ustalić, czy użytkownik jest botem (np. z użyciem sieci, urządzenia, odcisków JavaScript). Dla zapewnienia maksymalnej dokładności działania tych testów najlepiej jest zintegrować je z kompleksowym rozwiązaniem do zarządzania botami (patrz sekcja Wnioski).

Ogranicz częstotliwość, z jaką użytkownicy mogą żądać informacji

Ograniczanie częstotliwości żądań może być skuteczną techniką powstrzymywania mniej zaawansowanych botów. Ustawiając ścisłe limity liczby żądań, które adres IP może wysłać do Twojej witryny, zapobiegniesz wielu prostym atakom botów typu brute-force, polegającym na próbach logowania się przy użyciu tysięcy słów słownikowych i popularnych haseł. Współczesne, bardziej zaawansowane boty potrafią jednak utrzymywać liczbę zapytań tuż poniżej limitu częstotliwości, unikając wykrycia i nadal powodując szkody.

Prowadź szczegółowe dzienniki całego ruchu na stronie

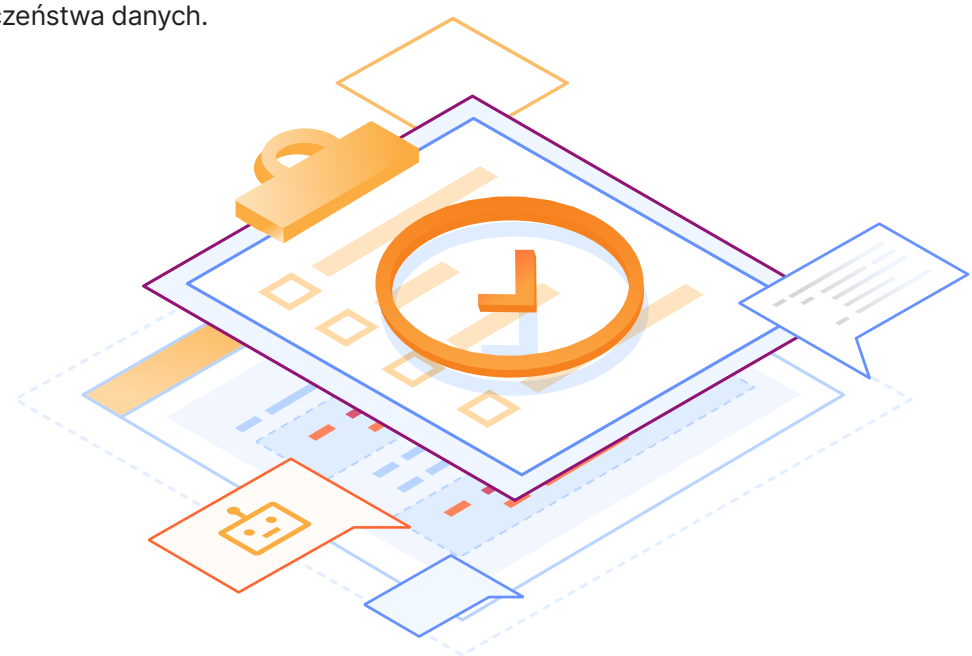
Choć prawdopodobnie prowadzisz już codzienne dzienniki wyświetleń stron i logowań do kont, bardziej szczegółowe rejestry informacji o użytkownikach — takie jak adresy IP, przeglądarki, urządzenia, systemy operacyjne, geolokalizacje, strony odsyłające, sieci i wyświetlenia stron — mogą okazać się nieocenione w wykrywaniu bardziej subtelnych wzorców aktywności. Dzienniki dają jasny obraz zachowania botów w witrynie, co umożliwia tworzenie skuteczniejszych zasad bezpieczeństwa. Ponadto dzienniki są często niezbędne do raportowania i zapewniania zgodności w przypadku wystąpienia naruszenia bezpieczeństwa danych.

Przekieruj boty do treści alternatywnej

Gdy masz pewność, że dane źródło ruchu to bot, podaj mu alternatywną treść, która zużywa jego zasoby obliczeniowe. Można nawet wprowadzać fałszywe dane — takie jak błędne informacje o cenach — do botów służących do pozyskiwania danych, czyniąc je bezużytecznymi dla ich operatorów. Tego typu techniki dadzą ci czas, aby obserwować zachowanie każdego bota, zrozumieć schemat jego aktywności i przygotować strategię, by raz na zawsze się z nim uporać.

Wymagaj dodatkowego uwierzytelnienia dla wszystkich użytkowników

W miarę jak ataki botów stają się coraz bardziej rozpowszechnione, coraz więcej witryn korzysta z zaostrzonych środków bezpieczeństwa, nawet w przypadku rzeczywistych logowań ludzi. Uwierzytelnianie dwuskładnikowe (2FA) wymaga na przykład od użytkowników potwierdzania tożsamości na wielu urządzeniach lub kontach, natomiast hasła jednorazowe (OTP) mogą zniechęcać boty wykorzystujące atak typu „credential stuffing”, utrudniając im włamanie się na konta. Należy jednak pamiętać, że techniki te mogą negatywnie wpłynąć na komfort użytkowania, powodując dodatkowe utrudnienia w procesie logowania.

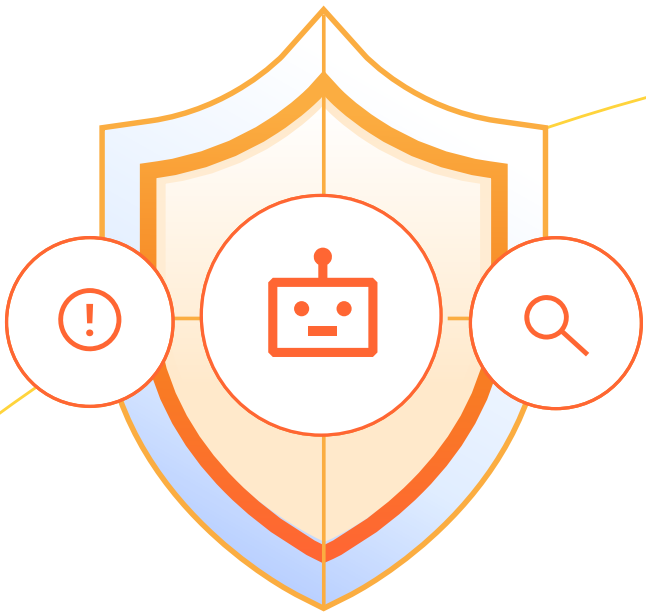


Wnioski

Analizując te taktyki, pamiętaj, że żadna z nich nie jest w stanie samodzielnie powstrzymać wszystkich botów. Dla zapewnienia firmie bezpieczeństwa prawdopodobnie konieczne będzie połączenie różnych taktyk, a także dodanie zaawansowanej analizy wielowymiarowych wzorców. Rozwiązanie Cloudflare Bot Management pomaga organizacjom z różnych branż we wdrożeniu tego wieloaspektowego podejścia. Jest ono włączone do rozległej sieci Cloudflare, która obsługuje miliony zasobów internetowych i obejmuje ponad 330 miast na całym świecie.

Dzięki ciągłej analizie zagrożeń z całej sieci rozwiązanie Cloudflare Bot Management zapewnia analizę behawioralną, uczenie maszynowe i identyfikację klienta po stronie użytkownika, co pozwala znacznie zredukować nakład pracy związany ze zwalczaniem złośliwych botów. Ponadto Cloudflare oferuje narzędzie Turnstile — doskonałe rozwiązanie zastępujące test CAPTCHA i służące do weryfikacji botów. Można je zintegrować z dowolną aplikacją internetową, dodając tylko kilka linijek kodu.

Dowiedz się więcej o rozwiązaniu Cloudflare Bot Management.



+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/pl-pl/

REV:BDES-6333.2024SEPT03